IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

HIKVISION USA, INC., and DAHUA TECHNOLOGY USA INC., *Petitioners*, v. FEDERAL COMMUNICATIONS COMMISSION and UNITED STATES OF AMERICA, *Respondents*.	Nos. 23-1032 & 23-1073

On Petition for Review of an Order of
the Federal Communications Commission

RESPONDENTS' OPPOSITION TO HIKVISION USA, INC.'S MOTION TO ENFORCE THE MANDATE

INTRODUCTION

Respondents the Federal Communications Commission and United States of America hereby oppose the motion of Petitioner Hikvision USA, Inc. to enforce the mandate of this Court in *Hikvision v. FCC*, 97 F.4th 938 (D.C. Cir. 2024). In *Hikvision*, the Court largely upheld a 2022 order in which the FCC implemented a statutory ban on the authorization of video surveillance and telecommunications equipment manufactured by certain Chinese-owned companies—including Hikvision—that pose

threats to national security. *Id.* at 948. By its terms, that ban applied only when the companies' video surveillance and telecommunications equipment was used for specified purposes, including for "physical security surveillance of critical infrastructure." *Id.* Although the Court upheld most aspects of the Commission's implementation of the statutory ban, it found the agency's interpretation of the phrase "critical infrastructure" overbroad. *Id.* The Court accordingly vacated that portion of the order and remanded for the agency to "comport its definition" with the statutory text. *Id.* at 950.

The Court's mandate issued on May 28, 2024. Now—just eight months later, and in the midst of a leadership transition at the FCC—Hikvision asks this Court to "enforce its mandate," Mot. 3, in two ways, neither of which deals with the agency's efforts to define the phrase critical infrastructure: First, Hikvision moves the Court to "requir[e] the agency to immediately lift [an administrative] freeze" that prevents Hikvision from submitting authorization applications for any equipment, including equipment Hikvision contends is not "covered" under the FCC's ban. Mot. 3. Second, Hikvision asks the Court to direct the Commission to act "within a set time" ("perhaps four months") on a compliance plan that Hikvision has submitted to the agency. Mot. 4.

The requested relief goes beyond the scope of this Court's mandate, which was limited to requiring the FCC to revise its definition of critical infrastructure. The Court did not direct the agency either to entertain equipment authorization requests from covered manufacturers or to approve those manufacturers' proposed compliance plans. Nor has Hikvision otherwise established a "clear and indisputable right" to relief as would be required to warrant a writ of mandamus. *E.g.*, *In re Trade & Com. Bank By & Through Fisher*, 890 F.3d 301, 303 (D.C. Cir. 2018). For these reasons, Hikvision's motion should be denied.

BACKGROUND

A. Statutory And Regulatory Background

In the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA), Congress prohibited federal agencies from using or procuring certain "covered" technology sold by Chinese companies. Pub. L. No. 115-232, § 889, 132 Stat. 1636, 1917–19 (2018). "The NDAA specifically targeted [Hikvision's] products for this limited ban from federal procurement," *Hikvision*, 97 F.4th at 941, and defined "covered telecommunications equipment" to include "video surveillance and telecommunications equipment produced by" Hikvision (and other specified companies) when that equipment is used "[f]or the purpose of

public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." NDAA § 889(f)(3).

In the Secure and Trusted Communications Networks Act, Pub. L. No. 116-124, 134 Stat. 158, Congress instructed the FCC to create a "Covered List" of equipment for which FCC subsidies could not be spent. 47 U.S.C. § 1601(a). Among other determinations, equipment was to be placed on that list if defined as "covered telecommunications equipment" under the NDAA. *Id.* § 1601(c)(3). Accordingly, the FCC published a Covered List that included Hikvision's "[v]ideo surveillance and telecommunications equipment" "to the extent [the equipment is] used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." *Public Safety and Homeland Security Bureau Announces Publication of the List of Equipment and Services Covered by Section 2 of the Secure Networks Act*, 36 FCC Rcd 5534, 5536 (2021); *see Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, 35 FCC Rcd 14284, 14316 ¶ 68 (2020) (*Supply Chain Second Order*).

In June 2021, the FCC proposed to ban the authorization of equipment on the Covered List under the Commission's equipment-authorization program. *Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program*, 36 FCC Rcd 10578, 10596 ¶ 40 (2021). Congress then passed the Secure Equipment Act, directing the Commission to "adopt rules in the proceeding initiated" in the notice of proposed rulemaking and requiring that the Commission "no longer review or approve any application for equipment authorization for equipment…on the [Covered List]." Pub. L. No. 117-55, 135 Stat. 423, § 2(a)(1), (2) (2021) (codified at 47 U.S.C. § 1601 note).

B. Equipment Authorization Process

Under the FCC's equipment authorization program, responsible parties, typically the equipment manufacturers, file applications for authorization with third parties known as "Telecommunications Certification Bodies" (TCBs), which the Commission has authorized to administer the certification process. *See Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program*, FCC 22-84 ¶ 50 (2022) (*Order*), reprinted at JA126–JA307. The FCC's Office of Engineering and

Technology (OET) oversees the process and provides guidance to applicants, TCBs, and test labs. *Id.* As part of the process, the FCC issues each producer a unique grantee code, to be used for each equipment authorization application. *See* 47 C.F.R. § 2.926(c)(1).

C. *Order* On Review

In the *Order* on review, the FCC banned the authorization of equipment on the Covered List. *See Order* ¶ 1 (JA127). Because the Covered List covers video surveillance and telecommunications equipment from Hikvision, and two other Chinese-owned companies, when used "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes," *Supply Chain Second Order* ¶ 68, the Commission prohibited authorizations to market and sell such equipment for those purposes, *see Order* ¶ 177 (JA195).

Because the companies' products are sold in the United States through independent dealers, the FCC observed that the companies "lack…oversight…over the marketing, distribution, and sales of their respective equipment." *Order* ¶ 180 (JA197). The Commission was "not confident that, absent additional prescriptive measures and Commission oversight, [the companies'] 'telecommunications equipment' or 'video

surveillance equipment' [would] not be marketed and sold for…purposes…prohibited under…the 2019 NDAA." *Id.* The *Order* therefore required that, before the FCC authorizes such equipment from these companies, they "each seek and obtain Commission approval for [their] respective plan[s]," to "ensure that such equipment will not be marketed or sold" for prohibited purposes. *Id.*

For the period between the adoption of the *Order* and the effective date of the agency's new rules, the Commission adopted an "interim freeze on further processing or grant of equipment authorization applications for equipment…produced by any entity identified on the Covered List." *Order* ¶ 264 (JA231). In adopting the freeze, the Commission provided that it would take effect immediately and last until the agency gave notice that the rules adopted in the *Order* had taken effect. *Id.*

The *Order* also included guidance about when equipment is used for "physical security surveillance of critical infrastructure." *Order* ¶ 209 (JA209). The Commission adopted the meaning of "critical infrastructure" provided in the USA Patriot Act of 2001, and it also found "that any systems or assets, physical or virtual, connected to the sixteen critical infrastructure sectors identified in [Presidential Policy Directive

21] or the 55 [national critical functions] identified in [a National Risk Management Center publication] could reasonably be considered 'critical infrastructure.'" *Id.* ¶ 212 (JA211).

D. This Court's Opinion

In challenging the Commission's *Order*, Hikvision and another Chinese-owned company, Dahua Technology USA Inc., argued that their products did not belong on the Covered List. This Court rejected that claim, explaining: "Congress has clearly expressed its view that [the companies'] products pose a risk to national security in certain circumstances." *Hikvision*, 97 F.4th at 945. "[T]o the extent…there [was] any ambiguity" regarding the extent of the companies' "threat to national security," moreover, the Court declined to "second-guess the FCC's judgment" underlying the *Order*. *Id.* at 948 (quoting *Pac. Networks Corp. v. FCC*, 77 F.4th 1160, 1164 (D.C. Cir. 2023)).

On the other hand, the Court agreed with the petitioners that the FCC's interpretation of "critical infrastructure" was "unjustifiably broad and…therefore arbitrary and capricious." *Hikvision*, 97 F.4th at 948. While the Commission's "choice of reference materials" was "reasonable" and "adequately explained," the Court held that the agency had "failed to explain or justify" a definition broadly encompassing all equipment

"connected to" the systems and assets identified in those materials. *Id.* at 949. The Court also held that the Commission's definition of "critical infrastructure" "fail[ed] to provide comprehensible guidance" to the petitioning companies, none of which could import or market video surveillance equipment without first "submit[ting] a marketing plan…demonstrat[ing] that their products [would] not be used" improperly. *Id.* at 950. "Without a clear understanding of what constitutes a 'connect[ion] to' critical infrastructure," the Court explained, the companies would "face significant difficulty in developing such…marketing plan[s]." *Id.* For these reasons, the Court "vacate[d] the portions of the FCC's order defining 'critical infrastructure' and remand[ed] to the Commission to comport its definition and justification for [that definition] with the statutory text of the NDAA." *Id.*

E. Hikvision's Proposed Compliance Plan

On August 7, 2023, while still challenging the FCC's definition of critical infrastructure before this Court, Hikvision also filed a compliance plan with the Commission, seeking to show how the company would comply with the *Order*'s restrictions. Hikvision proposed an internal policy that prohibited marketing specified equipment for a "Prohibited Purpose," and proposed to label such equipment with a warning against

use for "public safety, security of governmental facilities, physical security surveillance of critical infrastructure, and other national security purposes." *See* Mot. Ex. B at 11–12. In the proposed compliance plan, Hikvision offered its own definition of "critical infrastructure." *Id.* at 7.

As the proposal explains, Hikvision's equipment "is marketed, imported, sold, and distributed" in the United States "by a network of Distribution Partners," and Hikvision "does not collect or maintain records regarding the identity or location of the ultimate end user." Mot. Ex. B at 3. Thus, under the proposed plan, "[e]ach Distribution Partner [would] be responsible for ensuring its operations and activities comply" with the plan's marketing and sales prohibitions. *Id.*

On April 29, 2024—less than a month after this Court released its opinion in *Hikvision*, and before the mandate issued—Hikvision requested expedited approval of its proposed compliance plan. Mot. Ex. E. Hikvision argued that, instead of conducting a rulemaking proceeding to respond to the Court's remand regarding critical infrastructure, the FCC should address the issue "in the context of [Hikvision's] pending Compliance Plan." Mot. Ex. E at 2.

On August 28, 2024, counsel for Hikvision met with FCC staff to "provide[] an overview of Hikvision's compliance plan, and the policies and procedures designed to ensure compliance with the Commission's prohibitions on marketing and selling covered equipment for prohibited purposes." Mot. Ex. A at 8. Subsequent correspondence describes "a number of follow-ups that [Hikvision] took from [the] meeting," including "questions related to how [Hikvision] would fill in the details on monitoring end user compliance" and questions about "component parts" of products. Correspondence between D. Shaffer, FCC OET, and J. Nakahata, Counsel to Hikvision (Sept. 26, 2024), Mot. Ex. A at 37.

In an October 2, 2024, meeting with legal advisors to the FCC's then-Chairwoman, Hikvision's counsel sought additional guidance to design the plan's "monitoring activities," related to "operational post-sale oversight mechanisms regarding compliance." Mot. Ex. A at 10.

F. Further Developments

Interim Freeze Expires. On February 6, 2023, the rules adopted in the *Order* were published in the Federal Register, which gave notice that the rules had taken effect. *See Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program*, 88 Fed. Reg. 7592-01, 7593 (Feb. 6, 2023). The

interim freeze on authorization of all Hikvision products thus ended. *See Order* ¶ 264 (JA231). Because Hikvision did not yet have an approved compliance plan, however, authorization of any telecommunications or video surveillance equipment produced by the company was not yet permitted. *See id.* ¶ 180 (JA197); *see also Hikvision*, 97 F.4th at 950.

Hikvision Complains That It Cannot Submit Authorization Applications. On July 30, 2024, the FCC received an inquiry stating that a Hikvision subsidiary was interested in seeking authorization of a mobile robot that the subsidiary claimed was not "telecommunications equipment" or "video surveillance equipment." Mot. Ex. A at 23. FCC staff replied that, because Hikvision lacked a Commission-approved compliance plan, the company and its subsidiaries could not then "obtain an authorization for ANY telecommunications or video surveillance equipment." *Id.*

At Hikvision's October 2 meeting with the then-Chairwoman's legal advisors, Hikvision's representatives asserted that the company lacked "clarity as to the scope of covered 'video surveillance' and 'telecommunications' equipment." Mot. Ex. A at 11. In part for that reason, they complained that Hikvision was "unable to obtain equipment

authorizations on any of its equipment, including" purportedly non-covered equipment. *Id.*

Pens-Down Letter. On November 7, 2024, immediately following the presidential election, the ranking member of the Senate's Committee on Commerce, Science, and Transportation requested that the "FCC and all of its bureaus and offices immediately stop work on any partisan or controversial matters under consideration or in progress," in accordance with "norms set during past transfers of power." Letter from Senator Cruz to Chairwoman Rosenworcel (Nov. 7, 2024), attached as Ex. A.

Emergency Petitions. On December 16, 2024, Hikvision submitted an "emergency" request for the Commission to "promptly lift its freeze on the equipment authorization account" of Hikvision's parent company. Emergency Request for Commission Action on Hikvision's Equipment Authorization Account, ET Docket No. 21-232, at 1 (Dec. 16, 2024). That same date, Hikvision submitted a parallel "emergency" request for action on Hikvision's proposed compliance plan. Emergency Request for Commission Action on Hikvision's Compliance Plan, ET Docket No. 21-232, at 1 (Dec. 16, 2024). Hikvision warned that "[i]f the Commission [did] not act" on its requests "by January 15, 2025," Hikvision would seek relief from this Court. *Id.* at 1.

Leadership Transition. On January 20, 2025, with the resignation of then-Chairwoman Jessica Rosenworcel, President Trump designated FCC Commissioner Brendan Carr to become Chairman of the Commission.

ARGUMENT

A motion to enforce a judicial mandate under the All Writs Act is equivalent to a motion for mandamus. *See United States v. U.S. Dist. Court for S. Dist. of N.Y.*, 334 U.S. 258, 263–64 (1948); *In re Core Commc'ns, Inc.*, 531 F.3d 849, 855 (D.C. Cir. 2008). A party seeking to enforce a court's mandate "must show, as in all mandamus cases, (1) a clear and indisputable right to relief, (2) no other adequate means of redress, and (3) appropriateness under the circumstances." *In re Trade & Com.*, 890 F.3d at 303 (citing *Cheney v. U.S. Dist. Court for the Dist. of Columbia*, 542 U.S. 367, 380–81 (2004)). When a party seeking mandamus has no clear and indisputable right to relief, the court may "begin and end with the first" of the three mandamus requirements. *Id.*

That is the case here. Hikvision argues that the FCC has "flout[ed]" the Court's mandate in *Hikvision*, primarily because the Commission "maintain[s] that Hikvision cannot submit *any* new applications for approvals without a Compliance Plan in place," yet has not ruled on

Hikvision's pending compliance plan or lifted the freeze on its grantee code. Mot. 17. As explained further below, however, the Court in *Hikvision* nowhere addressed any duty the Commission might have with respect to Hikvision's compliance plan, nor did it direct the agency to resume processing Hikvision's equipment authorization applications.

To be sure, the Court remanded to the Commission to "comport its definition [of critical infrastructure] and justification for it with the statutory text of the NDAA." 97 F.4th at 950. Hikvision asserts in passing that "the Commission has taken *no* action whatsoever in response to [that] requirement." Mot. 17. But the issue on remand is complex and sensitive. Particularly given the transition in leadership at the agency, there has been no delay sufficiently "egregious" to justify mandamus under this Court's precedents. *Telecomm. Research & Action Ctr. v. FCC*, 750 F.2d 70, 79 (D.C. Cir. 1984) (*TRAC*).

I. THE COURT DID NOT ORDER THE COMMISSION TO PROCESS NEW APPLICATIONS FROM COMPANIES ON THE COVERED LIST.

Hikvision contends (Mot. 16–20) that "[t]his Court struck down the Commission's across-the-board ban on new approvals of Hikvision equipment as overbroad *and* acknowledged the time sensitivity of correcting that error." Mot. 18. It bases this claim in part on this Court's

finding that the Commission's definition of "critical infrastructure" was overbroad. *See id.* But the Court's holding that the Commission had not adequately "explain[ed] why everything 'connected to' any sector or function that implicates national security must be considered 'critical,'" *id.* (quoting *Hikvision*, 97 F.4th at 949–50), is not reasonably interpreted as a mandate that the Commission begin processing equipment applications from Hikvision or other companies on the Covered List before concluding the remand proceeding. To the contrary, this Court recognized that a valid interpretation of "critical infrastructure" was a necessary precedent to a compliance plan and equipment authorization. 97 F.4th at 950.

Hikvision argues that, because the Court "*vacat[ed]* the Commission's definition" of critical infrastructure "rather than simply remanding, the Court made clear that[,] pending a new justification by the Commission," the agency would be required to begin processing new equipment authorization applications from covered companies. Mot. 19. But that does not follow. Regardless whether the Court vacated the definition of critical infrastructure, or simply remanded for further explication, that was the only portion of the *Order* the Court found unlawful. The Court did *not* vacate the requirement that Hikvision must

have in place an approved compliance plan before the FCC will authorize its telecommunications or video surveillance equipment. *See Order* ¶ 180 (JA197). That requirement thus remains in effect.

In addition, Hikvision is wrong that the Commission has imposed an indefinite "across-the-board ban on new approvals of Hikvision equipment." *E.g.*, Mot. 18. To be sure, there is currently a freeze on Hikvision's applications because—as this Court has recognized, *Hikvision*, 97 F.4th at 950—Hikvision may not obtain an authorization for any telecommunications or video surveillance equipment without an approved compliance plan in place to ensure the equipment will not be used for physical security surveillance of critical infrastructure. Mot. Ex. A at 23; *accord Order* ¶ 180 (JA197). To effectuate that safeguard, FCC staff have, to date, declined to unlock Hikvision's grantee code, which prevents Hikvision from submitting any applications for equipment authorization—including for equipment the company believes should not be categorized as "telecommunications or video surveillance equipment." Mot. 8. But that staff-level action, which Hikvision has discussed in ex parte meetings, *see* above at 12–13, and as to which deliberation is ongoing, is not reasonably construed as evidence that the Commission has decided to put in place an indefinite, across-the-board freeze.

Hikvision contends otherwise on the theory that it cannot obtain authorization for equipment that it claims is "not even arguably" telecommunications or video surveillance equipment. Mot. 8. But the question whether Hikvision products are, or are not, video surveillance equipment is not so straightforward.

In its present motion, Hikvision asserts that "products like vacuum cleaners" cannot plausibly be categorized as "video surveillance equipment." Mot. 8. It similarly claims that "a mobile robot…used for moving items within a warehouse…is [not] covered equipment." *Id.* at 13.

In earlier submissions to the Commission, by contrast, Hikvision acknowledged that the categorization of such equipment is unclear. For example, in a request for clarification submitted to the agency on October 17, 2023, Hikvision described a robot vacuum that it recognized at least "arguably" fell "within the *Order*'s overly broad definition of video surveillance equipment," *Request for Clarification* at 2, attached as Ex. B, because the vacuum contained a camera, had Wi-Fi capability, and was capable of remote operation, *see id.* at 4. More recently, in a letter dated October 8, 2024, Hikvision described a warehouse robot that it urged the Commission not to treat as "video surveillance equipment," but

which it acknowledged had cameras and Wi-Fi capability. Mot. Ex. A at 24–25.

Given the broad definition of "video surveillance equipment" adopted in the *Order*—which Hikvision has not and does not challenge before this Court—it is, at a minimum, unclear whether the products Hikvision describes (Mot. 8) fall within that category. Hikvision thus does not have a "clear and indisputable" right, *Cheney*, 542 U.S. at 381, to immediately seek authorization for the products that it asserts are not "video surveillance equipment." Again, Hikvision has discussed these issues with FCC staff and former leadership, *see* above at 12–13, and deliberation is ongoing. Given the "importance" of guarding against the authorization of "equipment that poses an unacceptable risk to national security," *Order* ¶ 204 (JA207), Hikvision is not entitled to an order from this Court directing the Commission to "immediately lift the freeze" on Hikvision's grantee code, Mot. 22.

II. THE COURT DID NOT ORDER THE COMMISSION TO ADJUDICATE HIKVISION'S COMPLIANCE PLAN.

Hikvision does not (and could not) assert that *Hikvision* directed the Commission to adjudicate Hikvision's compliance plan. Although Hikvision had submitted that plan to the agency before the Court issued

its opinion, *see* above at 9–11, the plan was not a subject of briefing or argument, and the Court's opinion does not address it. There is thus no basis for this Court to direct the FCC to "act promptly" on Hikvision's proposed compliance plan. Mot. 22.

Indeed, it is not feasible to determine that an equipment manufacturer's plan will ensure compliance with the prohibition against surveillance of "critical infrastructure" until the FCC better defines what that term means in the first place. *Hikvision*, 97 F.4th at 950. Nonetheless, the FCC has not sat on its hands. Both FCC staff and leadership have met with the company's counsel to discuss Hikvision's compliance plan, and the agency has indicated that an acceptable plan would require Hikvision to play a more active role in ensuring that its products are not used for prohibited purposes. *See* Mot. Ex. A at 10 (discussing staff guidance requiring "monitoring activities," related to "operational post-sale oversight mechanisms regarding compliance"); Mot. Ex. A at 37 (correspondence regarding "details on monitoring end user compliance"). After all, the *Order* required compliance plans because the companies "lack[ed] oversight" over the actual marketing and sale of their equipment in the United States by independent distributors. *Order* ¶ 180 (JA197). Hikvision's proposed plan nevertheless relies on "[e]ach

Distribution Partner [to] be responsible for ensuring its operations and activities comply." Mot. Ex. B at 3. The ongoing dialogue between the Commission and Hikvision on Hikvision's proposal has been necessary and productive, and the Commission is not fairly accused (Mot. 17) of unreasonable delay.

In tacit recognition that the mandate in *Hikvision* had nothing to do with its compliance plan, Hikvision argues that "approval of" the plan would be the "most expeditious way" for the Commission "to address this Court's remand as to the scope of 'critical infrastructure.'" Mot. 11. But the Court did not direct that approach. *N. Carolina Fisheries Ass'n, Inc. v. Gutierrez*, 550 F.3d 16, 20 (D.C. Cir. 2008) ("when a court…determines that an agency made an error of law, the court's inquiry is at an end," and "[o]nly in extraordinary circumstances do [courts] issue detailed remedial orders"). Moreover, "Congress has granted the Commission broad authority, to 'conduct its proceedings in such manner as will best conduce to the proper dispatch of business and to the ends of justice.'" *China Telecom (Americas) Corp. v. FCC*, 57 F.4th 256, 268 (D.C. Cir. 2022) (quoting 47 U.S.C. § 154(j)). Accordingly, while Hikvision would prefer that the Commission adjudicate its individual compliance plan, instead of conducting notice-and-comment rulemaking, the Commission

has no "clear and indisputable" duty to adopt Hikvision's preferred approach. Especially when the interpretation of critical infrastructure offered in Hikvision's proposed compliance plan does not cite any independent source (let alone the authorities on which the Commission reasonably relied on in the *Order*, *see Hikvision*, 97 F.4th at 949), the agency may reasonably prefer to explicate "critical infrastructure" in a notice-and-comment rulemaking. *See In re Monroe Commc'ns Corp.*, 840 F.2d 942, 946 (D.C. Cir. 1988) (denying mandamus and noting that courts "must give agencies great latitude in determining their agendas").

III. THERE HAS BEEN NO UNREASONABLE DELAY IN REVISING THE DEFINITION OF "CRITICAL INFRASTRUCTURE."

Hikvision's passing complaint that "the Commission has taken *no* action whatsoever in response to this Court's requirement to provide a 'comprehensible standard' for critical infrastructure," Mot. 17, likewise does not justify mandamus relief.

This Court will grant mandamus for agency action "unreasonably withheld," 5 U.S.C. § 706(1), but only where delay is "egregious." *TRAC*, 750 F.2d at 79. Under *TRAC*, among other factors, the Court considers a "rule of reason" to evaluate the causes and length of agency delay. *Id.* at 80 (quotation marks and citation omitted). For example, the Court has

denied mandamus regarding a contested licensing renewal that took over five years, because the matter was "a delicate one," requiring the FCC to balance competing concerns. *Monroe Commc'ns Corp.*, 840 F.2d at 945–46. Where this Court has granted mandamus, delays have routinely lasted four years or more. *See In re Am. Rivers & Idaho Rivers United*, 372 F.3d 413, 418 (D.C. Cir. 2004) (six-year delay); *MCI Telecommunications Corp. v. FCC*, 627 F.2d 322 (D.C. Cir. 1980) (four-year delay). In *In re Core Communications, Inc.*, 531 F.3d 849, 857 (D.C. Cir. 2008), this Court originally remanded an FCC order for further justification, then denied mandamus after three years, and only granted mandamus after six years from the remand.

The agency's timeline here does not approach that level of delay. This Court entered its *Hikvision* opinion on April 2, 2024, and the mandate issued on May 28, 2024. Although the Commission has not yet taken any public next steps—beyond internal deliberations—responding to the Court's remand, that is understandable. As the history of this litigation makes plain, the definition of "critical infrastructure" is a complex and sensitive issue that demands careful consideration on the agency's part to revise. Immediately upon President Trump's election, the FCC received a congressional request to stop work on controversial

issues, and the agency has since undergone a transition in leadership. *See* above at 13. In these circumstances, it is not unreasonable that—roughly eight months from when the mandate in this case issued—the agency has not yet revised its definition of "critical infrastructure."[1]

[1] Zhejiang Dahua Technology Co., Ltd (Zhejiang Dahua), which at the time of the Court's decision was the parent company of petitioner Dahua USA, moved on February 7, 2025, to substitute itself for Dahua USA. That motion remains pending and the time for responses has not yet run. Earlier today, Zhejiang Dahua filed a "Response to [Hikvision's] Motion to Enforce the Mandate" and also "move[d] for affirmative relief," seeking for itself any relief applied to Hikvision. Zhejiang Dahua Mot. at 1, 3. Insofar as the Court may entertain Zhejiang Dahua's motion, we note that Zhejiang Dahua offers no substantive argument beyond what Hikvision has argued, and thus similarly has not justified the requested relief. In addition, Zhejiang Dahua has not even attempted to show that the FCC has unreasonably delayed action on a compliance plan, or that the company has sought approval for equipment that is not telecommunications or video surveillance equipment. To the extent Zhejiang Dahua's motion is procedurally proper, respondents reserve the right to respond within the time permitted under Fed. R. App. P. 27(a)(3).

CONCLUSION

For the foregoing reasons, Hikvision's motion to enforce the mandate should be denied.

Dated: February 10, 2025

Respectfully submitted,

/s/ Matthew J. Dunne

D. Adam Candeub
General Counsel

Jacob M. Lewis
Deputy General Counsel

Sarah E. Citrin
Deputy Associate General Counsel

Matthew J. Dunne
Counsel

FEDERAL COMMUNICATIONS COMMISSION
45 L Street NE
Washington, DC 20554
(202) 418-1740
fcclitigation@fcc.gov

Sharon Swingle
Casen Ross
Attorneys

U.S. DEPARTMENT OF JUSTICE
CIVIL DIVISION
950 Pennsylvania Ave. NW
Washington, DC 20530
Counsel for Respondent United States of America

CERTIFICATE OF COMPLIANCE

Certificate of Compliance With Type-Volume Limitation,
Typeface Requirements and Type Style Requirements

1. This document complies with the type-volume limit of Fed. R. App. P. 27(d)(2) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f) and D.C. Circuit Rule 32(e)(1):

   ☒ this document contains 4,595 words, *or*

   ☐ this document uses a monospaced typeface and contains ____ lines of text.

2. This document complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because:

   ☒ this document has been prepared in a proportionally spaced typeface using Microsoft Word for Office 365 in 14-point Century Schoolbook, *or*

   ☐ this document has been prepared in a monospaced spaced typeface using _____ with _____.

/s/ *Matthew J. Dunne*
Matthew J. Dunne
Counsel for Respondent
Federal Communications Commission